National Security Agency/Central Security Service

INFORMATION
ASSURANCE
DIRECTORATE

CGS Hardward Device Inventory Capability

Version 1.1.1

Hardware Device Inventory provides the Enterprise with the methods and schema necessary to identify and track its classified and unclassified hardware assets, including operational assets and spares.

07/30/2012

CGS Hardware Device Inventory Capability

Version 1.1.1

Table of Contents

1 Revisions

Name	Date	Reason	Version
CGS Team	30 June 2011	Initial release	1.1
CGS Team	30 July 2012	Inclusion of new IAD document template & Synopsis	1.1.1

2 Capability Definition

The Capability definition provides an understanding of the importance of the Capability to the Enterprise. It provides a high-level overview of the Capability based on definitions derived from Committee on National Security Systems (CNSS) Instruction No. 4009.

Hardware Device Inventory provides the Enterprise with the methods and schema necessary to identify and track its classified and unclassified hardware assets, including operational assets and spares. Maintaining a Hardware Device Inventory means to identify the hardware as well as its components. Hardware shall include components such as network interface cards (NICs), telecom devices, network devices, and hard drives.

3 Capability Gold Standard Guidance

The Capability Gold Standard Guidance evaluates the Enterprise needs and overlays the expected Gold Standard behavior. The guidance goes beyond the concept of “good enough” when describing the Gold Standard recommendations, considers industry best practices, and describes a level of security that not only meets current standards but also exceeds them across the Enterprise.

The Hardware Device Inventory Capability is used to maintain a complete, consolidated, accurate, scalable, and up-to-date database of all hardware and hardware components in use by an Enterprise or network based on mission needs. This inventory includes workstations, servers, peripheral devices, network appliances, telecommunications equipment, other discoverable devices, and any hardware customizations that have occurred to render systems different from their baseline configuration. Hardware includes anything residing on the network or that can be connected to the network, which may have security implications, including operational assets and spares. Different hardware devices have different capabilities and characteristics, which the inventory captures based on type of device. Data stored about each hardware device shall include information such as ownership, description, version, installation date, baseline, vendor object identifier, licenses, known vulnerabilities, and/or compatibility issues.

The Hardware Device Inventory Capability shall contain an identification schema for uniquely naming hardware assets. The asset’s naming schema shall not be associated with the agency or mission support needs but shall contain a method to link physical inventory finding to the software-based inventory.

The asset database for the Hardware Device Inventory shall be scalable, and stored and maintained centrally. If the information is not available for a particular asset, the Enterprise responsible for that asset shall be responsible for capturing and documenting the available information and providing exceptions, in the case of extremely sensitive, compartmented hardware, on an as-needed basis. The information included in the identification schema shall depend on what information the Configuration Management Capability needs for baseline tracking.

The Hardware Device Inventory Capability shall have accountability for all hardware device assets. All hardware assets in the hardware inventory shall be held in an asset database. Some hardware devices may require licensing for their use; therefore, any relevant licenses or license keys shall be noted in the inventory. The licenses and/or key shall be protected by employing other Capabilities such as Physical and Environmental Protections, System Protection, and/or Data Protection. The Configuration Management Capability will enforce the use of the licenses or keys as part of maintaining the baseline.

The process of populating a Hardware Device Inventory shall be as automated as possible. It is accepted that some functions may require human interaction, but the majority of the functions performed by this Capability shall be automated. All online hardware shall have a real-time feed to the inventory. Offline hardware components shall be inventoried by date and status (i.e., whether hardware components are checked-in or checked-out).

The Hardware Device Inventory Capability provides a near real-time account of discoverable hardware in the environment and up-to-date inventory of hardware spares. This information is housed in the asset database. The Configuration Management Capability shall monitor the database, and subsequent inventories within, for changes as well as version or other information about the hardware assets. This information will be used by the Configuration Management Capability to determine compliance with the appropriate baseline. Configuration Management shall be responsible for the identification and removal of unauthorized hardware from the deployed hardware asset.

Verification of the Hardware Device Inventory shall provide verification of what is expected (asset database Hardware Device Inventory) versus what exists on the network (near real-time or up-to-date inventories based on scanning or manual checks). In some cases verification or auditing of the asset database and inventory shall be carried out by external sources. Anything residing on the network or that can be connected to the network and has security implication shall be inventoried within a recurring timeframe commensurate with the level of risk the hardware device components may pose if lost, compromised, or used improperly. Policy shall dictate periodic or recurring inventory activities as well as reporting requirements for the inventory.

The Hardware Device Inventory shall indicate hardware association with an accredited system. When a change to an inventory hardware device item occurs, automated notification shall be sent to the system owner(s) for the associated accredited system so that updates can occur to the system security plans (SSP) or subsequent security documentation. Changes to the inventory are recorded and sent to the Enterprise Audit Management Capability. Inventory reduction is driven by mission needs and is part of system decommissioning (see the Decommission Capability).

4 Environment Pre-Conditions

The environment pre-conditions provide insight into environmental, user, and technological aspects needed for Capability implementation. These pre-conditions are services or other Capabilities that must be in place within the Enterprise for the Capability to function.

1. All hardware devices with network connectivity are configured to be discoverable and are assigned a unique identifier, which is able to be automatically correlated with an automatically discoverable identifier.
2. Baselines are established but may not be the same for the same type of hardware devices (depending on Organization and mission hardware device, baselines may differ for the same type hardware).
3. Necessary Physical and Environmental Protections are documented, audited, and employed within the environment.
4. Approved hardware is procured and licenses are obtained during the acquisition process.

5 Capability Post-Conditions

The Capability post-conditions define what the Capability will provide. They define functions that the Capability will perform or constraints that the Capability will operate under when performing its function.

1. The Capability maintains a log of hardware changes on both a per-baseline and per-device basis.

2. The Capability maintains an inventory of all hardware assets including operational and spare.
3. The Capability maintains information on the physical location of hardware assets.

6 Organizational Implementation Considerations

Organizational implementation considerations provide insight into what the Organization needs to establish, ensure, and have in place for the specified Capability to be effective. It provides guidance specific to the actions, people, processes, and departments that an Organization will need to execute or establish to implement the guidance described in Section 3 (Capability Gold Standard Guidance).

Organizations will provide a mechanism for tracking all hardware device assets' origin and functionality, and use within the Enterprise, to comply with supporting the mission needs of the Enterprise. In addition, Organizations will determine what hardware information is maintained in their asset database, such as how the inventory is populated, where the inventory is located, and the tradeoff between dollar value, risk, and devices to be tracked. Only authorized personnel and processes will be granted access to modify or use the database.

Organizations will be responsible for determining the naming schema of the hardware assets, which will indicate the hardware and version of assets. Hardware Device Inventory assets will have a unique nomenclature to identify the hardware in the inventory.

Organizations will ensure that coordination with other Capabilities, such as the Configuration Management, Network Mapping, and the Software Inventory Capabilities, is employed to assist in maintaining an accurate depiction of all hardware devices in the inventory. Organizations will maintain hardware asset information in their asset database while actual hardware assets and their licenses and license keys will be stored in the Hardware Device Repository (as part of the Configuration Management Capability).

The Organization will employ industry standard tools and formats to conduct automated inventory collection. In addition, when selecting a tool, consideration will be given to the relationship between the Hardware Device Inventory Capability and other Capabilities.

Organizations will be responsible for periodically auditing the Hardware Device Inventory for accuracy and compliance with relevant management policies. Inaccuracies in the inventory will be corrected, and a reasonable effort will be made to determine the inaccuracy origin and whether it is the result of a recurring or singular problem. The frequency of these audits will vary for each Organization or network.

7 Capability Interrelationships

Capability interrelationships identify other Capabilities within the Community Gold Standard framework that the Capability in this document relies on to operate. Although there are many relationships between the Capabilities, the focus is on the primary relationships in which the Capabilities directly communicate with or influence one another.

7.1 Required Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are necessary for the Capability in this document to operate.

- Understand Mission Flows–The Hardware Device Inventory Capability relies on the Understand Mission Flows Capability to provide mission information that is used for asset management purposes.
- Understand Data Flows–The Hardware Device Inventory Capability relies on the Understand Data Flows Capability to provide data flow information for asset management purposes.
- Software Inventory–The Hardware Device Inventory Capability relies on the Software Inventory Capability to provide information used to track which hardware and software assets are associated.
- Deployment–The Hardware Device Inventory Capability relies on the Deployment Capability to provide information about hardware systems that are deployed.
- Decommission–The Hardware Device Inventory Capability relies on the Decommission Capability to report changes in the ownership of assets.

7.2 Core Interrelationships

The following Capability interrelationships include the Capabilities within the Community Gold Standard framework that relate to every Capability.

- Portfolio Management–The Hardware Device Inventory Capability relies on the Portfolio Management Capability to determine current and future investment needs and prioritize investments based on those needs.
- IA Policies, Procedures, and Standards–The Hardware Device Inventory Capability relies on the IA Policies, Procedures, and Standards Capability to

provide information about applicable federal laws, Executive Orders, regulations, directives, policies, procedures, and standards.

- IA Awareness–The Hardware Device Inventory Capability relies on the IA Awareness Capability for an awareness program to inform personnel of their responsibilities related to IA.
- IA Training–The Hardware Device Inventory Capability relies on the IA Training Capability to provide training programs related to IA activities in accordance with agency policies.
- Organizations and Authorities–The Hardware Device Inventory Capability relies on the Organizations and Authorities Capability to establish the relevant roles and responsibilities.

7.3 Supporting Interrelationships

The following Capability interrelationships include the other Capabilities within the Community Gold Standard framework that are not necessary for the Capability to operate, although they support the operation of the Capability in this document.

- Network Mapping–The Hardware Device Inventory Capability relies on the Network Mapping Capability to provide a graphical representation of the location of hardware assets.
- System Protection–The System Protection Capability provides protections for the devices monitored by the Hardware Device Inventory.
- Physical and Environmental Protection–The Hardware Device Inventory Capability relies on the Physical and Environmental Protection Capability to provide protections to all Enterprise assets including hardware in operational or spare status.
- Data Protection–The Hardware Device Inventory Capability relies on the Data Protection Capability to provide protection measures to safeguard hardware device information.
- Network Security Evaluations–The Hardware Device Inventory Capability relies on the Network Security Evaluations Capability to supply information that is used to fill any gaps that may exist in the inventory.
- Risk Mitigation–The Hardware Device Inventory Capability implements individual countermeasures that may be selected by the Risk Mitigation Capability.
- Acquisition–The Hardware Device Inventory Capability relies on the Acquisition Capability to provide information about hardware devices as soon as they are acquired by the Enterprise so that they can be monitored.

8 Security Controls

This section provides a mapping of the Capability to the appropriate controls. The controls and their enhancements are granularly mapped according to their applicability. In some instances, a control may map to multiple Capabilities.

Control Number/Title	Related Text
NIST SP 800-53 Revision 3, *Recommended Security Controls for Federal Information Systems and Organizations*	
CM-8 *INFORMATION SYSTEM COMPONENT INVENTORY*	Control: The organization develops, documents, and maintains an inventory of information system components that: a. Accurately reflects the current information system; b. Is consistent with the authorization boundary of the information system; c. Is at the level of granularity deemed necessary for tracking and reporting; d. Includes [Assignment: organization-defined information deemed necessary to achieve effective property accountability]; and e. Is available for review and audit by designated organizational officials. Enhancement/s: (1) The organization updates the inventory of information system components as an integral part of component installations, removals, and information system updates. (2) The organization employs automated mechanisms to help maintain an up-to-date, complete, accurate, and readily available inventory of information system components. (3) The organization: (a) Employs automated mechanisms [Assignment: organization-defined frequency] to detect the addition of unauthorized components/devices into the information system.
PM-5 *INFORMATION SYSTEM INVENTORY*	Control: The organization develops and maintains an inventory of its information systems. Enhancement/s: None Specified.

9 Directives, Policies, and Standards

This section identifies existing federal laws, Executive Orders, regulations, directives, policies, and standards applicable to the Capability but does not include those that are agency specific.

Hardware Device Inventory Directives and Policies Directives and Policies

Title, Date, Status	Excerpt / Summary
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
NSPD-54/HSPD-23 Cybersecurity Presidential Directive (Comprehensive National Cybersecurity Initiative [CNCI]), 8 January 2008, Classified	Summary: National Security Presidential Directive-54/Homeland Security Presidential Directive-23 (NSPD-54/HSPD-23), in which the Comprehensive National Cybersecurity Initiative (CNCI) is described, is classified. Initiative 7 deals with increasing the security of classified networks.
Department of Defense (DoD)	
DoDI 8100.3 Department of Defense (DoD) Voice Networks, 16 January 2004, Unclassified	Summary: This instruction requires "... Conduct, with the DoD Components, an annual inventory of DSN and DRSN telecommunications...a single comprehensive DoD inventory of telecommunications switches...DSN and DRSN and submit this inventory to the ASD (NII)/DoD CIO...accreditation data on software and hardware of all telecommunications..."
CJCSI 6510.01E, Information Assurance (IA) and Computer Network Defense, 12 August 2008, Unclassified	Summary: This instruction requires a current and comprehensive baseline inventory of hardware and software.
Committee for National Security Systems (CNSS)	
CNSSP-17 Policy on Wireless Communications: Protecting National	Summary: This policy to help agencies better safeguard National Security Information (NSI) during wireless transmission and delivery, while stored on mobile systems, and while stored on fixed systems that can be accessed by

Security Information, May 2010, Classified	wireless media. It addresses the use of wireless technologies in areas where NSI is discussed or processed.
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Hardware Device Inventory Standards

Title, Date, Status	**Excerpt / Summary**
Intelligence Community (IC)	
Nothing found	
Comprehensive National Cybersecurity Initiative (CNCI)	
Nothing found	
Department of Defense (DoD)	
Nothing found	
Committee for National Security Systems (CNSS)	
Nothing found	
Other Federal (OMB, NIST, …)	
Nothing found	
Executive Branch (EO, PD, NSD, HSPD, …)	
Nothing found	
Legislative	
Nothing found	

Other Standards Bodies (ISO, ANSI, IEEE, …)	
RFC 2263 – SNMPv3 Applications, Unclassified	Summary: This memo describes five types of Simple Network Management Protocol (SNMP) applications that use an SNMP engine as described in Request for Comments (RFC) 2261. The types of application described are Command Generators, Command Responders, Notification Originators, Notification Receivers, and Proxy Forwarders. SNMPv3 uses the User-based Security Model (USM) for message security and the View-based Access Control Model (VACM) for access control. USM specifies authentication and encryption. VACM specifies access-control rules.
IETF RFC 4122- UUID, Unclassified	Summary: This document provides guidance on creating unique identifiers.

10 Cost Considerations

This section provides examples of some of the types of costs that the Organization will need to consider when implementing this Capability. The following examples are costs that are common across all of the Community Gold Standards Capabilities:

1. Solution used for implementation (hardware and/or software)
2. Necessary training
3. Licensing (if applicable)
4. Lifecycle maintenance
5. Impact/dependency on existing services
6. Manpower to implement, maintain, and execute
7. Time to implement, maintain, and execute
8. Network bandwidth availability and consumption
9. Scalability of the solution relative to the Enterprise
10. Storage and processing requirements

In addition to the common costs, the following are examples of cost considerations that are specific to this Capability:

1. Storage requirements–The Capability will need a capacity to store data about hardware devices, which may need to be segregated on a separate network (out of band). In addition, the Enterprise will need to provide for the physical storage of hardware.

2. Lifecycle maintenance–The Capability will need to monitor spare parts as they become available and are put into use.

11 Guidance Statements

This section provides Guidance Statements, which have been extracted from Section 3 (Capability Gold Standard Guidance) of this Capability document. The Guidance Statements are intended to provide an Organization with a list of standalone statements that are representative of the narrative guidance provided in Section 3. Below are the Guidance Statements for the Hardware Device Inventory Capability.

- The Enterprise shall use a hardware device inventory to maintain a comprehensive, consolidated, accurate, scalable, and up-to-date database of all hardware and hardware components in use by the Enterprise or network, based on mission needs.
- The hardware device inventory shall include workstations, servers, peripheral devices, network appliances, telecommunications equipment, other discoverable devices, and any hardware customizations that have occurred that render systems different from their baseline configuration.
- Different hardware devices have different capabilities and characteristics, which the hardware device inventory shall capture based on the type of device.
- Data stored by the hardware device inventory about each hardware device shall include information such as ownership, description, version, installation date, baseline, vendor object identifier, licenses, known vulnerabilities, and/or compatibility issues.
- The hardware device inventory shall contain an identification schema for uniquely naming hardware assets.
- The Enterprise shall use an asset-naming schema for its hardware device inventory that is not associated with the agency or mission support needs.
- The hardware device inventory shall contain a method to link physical inventory to assets in the software inventory.
- The hardware device inventory shall be scalable.
- The hardware device inventory shall be stored and maintained centrally.
- The hardware device inventory shall provide exceptions for assets that deviate from inventory policies, such as with extremely sensitive or compartmented hardware, on an as-needed basis.
- All information stored in the hardware device inventory that is included for the identification schema shall be baseline trackable for configuration management needs.

- The Enterprise shall have accountability for all hardware device assets.
- All hardware assets in the hardware inventory shall be held in an asset database, including any applicable licenses or license keys.
- The hardware device inventory shall leverage other Enterprise systems, as appropriate, to protect licenses and/or keys.
- The hardware device inventory shall ensure that the Enterprise configuration management process enforces the use of licenses or keys as part of maintaining the baseline.
- The Enterprise shall automate the process of populating the hardware device inventory, as possible.
- All online hardware shall have a real-time feed to the hardware device inventory.
- The hardware device inventory shall monitor offline hardware components by date and status (i.e., whether hardware components are checked-in or checked-out).
- The Enterprise shall employ configuration management to monitor the hardware device inventory database, and subsequent inventories within, for changes including version and other information about the hardware assets.
- The Enterprise configuration management system shall use configuration information from the hardware device inventory to determine device compliance with appropriate baselines.
- The Enterprise shall employ configuration management to identify and remove unauthorized hardware from deployed hardware assets.
- The Enterprise shall provide verification of the assets in the hardware device inventory to identify the differences of what is expected (asset database) versus what exists on the network (near real-time or up-to-date inventories based on scanning or manual checks).
- External sources shall be allowed to carry out verification or auditing of the hardware device inventory, if needed.
- All hardware device assets shall be inventoried within a recurring timeframe commensurate with the level of risk the hardware device components may pose if lost, compromised, or used improperly.
- Policy shall dictate periodic or recurring inventory activities as well as reporting requirements for the hardware device inventory.
- The hardware device inventory shall indicate hardware association with an accredited system.
- When a change occurs to an asset in the hardware device inventory, automated notification shall be sent to the system owner(s) for the associated accredited

system so that updates can occur to the SSP or subsequent security documentation.

- All changes to the hardware device inventory shall be recorded in accordance with the Enterprise audit system.